The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
8/11/2009

SUBJECT:
Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution (MS09-044)

OVERVIEW:
Vulnerabilities have been discovered in the Microsoft Remote Desktop Connection which could allow an attacker to take complete control of an affected system. The Microsoft Remote Desktop Connection is a client application which uses the Remote Desktop Protocol (RDP) to connect to a computer for remote access and is inluded by default with Microsoft Windows installations. Exploitation occurs if a user uses Microsoft Remote Desktop Connection to connect to a malicious RDP server, or if a user visits a specially crafted web page or opens a malicious e-mail attachment which is specifically crafted to take advantage of these vulnerabilities. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

Windows 2000 Service Pack 4
Windows XP Service Pack 2
Windows XP Service Pack 3
Windows Server 2003 Service Pack 2
Windows Vista Service Pack 1
Windows Vista Service Pack 2
RDP Version 5.0
RDP Version 5.1
RDP Version 5.2
RDP Version 6.1
Remote Desktop Connection Client for Mac 2.0

RISK:

Government:
Large and medium government entities: High
Small government entities: High

Businesses:
Large and medium business entities: High
Small business entities: High

Home users: High

DESCRIPTION:
Two vulnerabilities have been discovered in the Microsoft Remote Desktop Connection which could allow an attacker to take complete control of an affected system. Both vulnerabilities are a result of an insufficient parameter validation, and lead to a heap overflow. The first vulnerability occurs when a user connects to a malicious RDP server. The second vulnerability occurs when a user visits a malicious webpage or opens a malicious e-mail attachment which instantiates the vulnerable ActiveX component. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:
Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/Bulletin/MS09-044.mspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1133
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1929

Security Focus:
http://www.securityfocus.com/bid/35973
http://www.securityfocus.com/bid/35971